CHAPTER

10

PERFORMANCE TUNING

After reading this chapter and completing the exercises, you will be able to:

- Create a performance baseline
- Understand the performance and monitoring tools found in Windows XP Professional
- Create a Counter log for historical analysis
- Create Alert events to warn of performance problems
- Detect and eliminate bottlenecks

Once you have installed and configured Windows XP Professional, connected it to the network and set up printers, you are ready to optimize your computer's performance. Windows XP includes several tools for monitoring your computer's performance and tuning it for the best output, including the Performance Console, Event Viewer, and Task Manager.

We introduce these tools and discuss specific system objects and counters that are worth monitoring. You learn what combinations of counters can be used to analyze system slowdowns and how to isolate, identify, and correct system bottlenecks. Very few operating systems include the kinds of tools that Windows XP Professional offers to help inspect and analyze system performance. In this chapter, you learn how to use these Windows XP Professional monitoring tools to good effect.

Establishing a Baseline

To recognize bottlenecks, it's first necessary to establish some feeling for what's normal on your system, a **baseline** against which you can measure system behavior. Key elements in a baseline include recorded observations about the characteristics and behavior of the computer system.

If you think back to the architectural overview of the Windows operating system in Chapter 1, "Introduction to Windows XP Professional," you should recall that Windows XP is an object-oriented operating system in which all user-accessible system resources, files, folders, processes, threads, and so forth take the form of specific object instances. In object-oriented parlance, **objects** have properties; in Windows operating systems, some of these properties are called **counters** because they count, average, or otherwise monitor specific events, activities, or behavior of the objects with which they're associated. Counters make it quite easy to gather data about the system while it's running and impose surprisingly little overall performance overhead on a system.

Baselines can be recorded by creating a Counter log for whatever list of performance object counters you consider important and collecting that data at regular intervals over a period of time. This helps you establish a definition of what a normal load looks like—which is what a baseline is supposed to convey—and provides points of comparison with future system behavior.

Of course, you'll want to make sure that your system baseline itself doesn't indicate existing bottlenecks. If you discover unacceptably long queues or evidence of memory problems when you create your baseline, you'll want to address these bottlenecks right away. We discuss how you can do this for common Windows XP Professional subsystems in the sections that follow.

Monitoring and Performance Tuning

When it comes to system analysis, there are two primary activities involved in tackling performance-related issues:

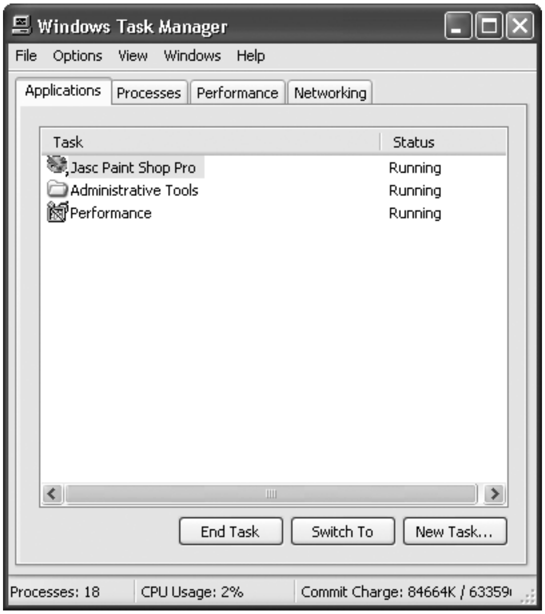
- *Monitoring:* Requires a thorough understanding of system components, their behavior, and how they interact, as well as continued observation of those components and how they behave on a regular (preferably scheduled) basis.
- *Performance tuning:* Consists of changing a system's configuration systematically and carefully observing performance before and after such changes. Changes that improve performance should be left in place; those that make no difference—or that make things worse—should be reversed. There are many ways to improve Windows XP Professional performance. The more useful approaches or configuration changes are covered in this chapter.

In many ways, Windows XP Professional does a remarkable job of tuning itself. It is capable of managing both its physical and virtual memory quite well. It also adjusts allocation of memory dynamically and effectively among a variety of uses, including file caching, virtual memory, system kernel, and applications. Because its self-tuning features manage resources so effectively, Windows XP Professional offers a more limited set of tools and utilities to monitor and alter system performance than do older operating systems, such as Windows NT. Changing the default Windows XP Professional operating system configuration is rarely required. Instead, you learn how to recognize and react to system bottlenecks that can limit a system's overall performance and respond to the need for tuning and manual optimization only when it's required.

Task Manager

Windows Task Manager, shown in Figure 10-1, provides an overview of the current state of a computer. You can access the Task Manager in one of three ways:

- Press Ctrl+Alt+Delete
- Press Ctrl+Shift+Esc
- Right-click any unoccupied area on the Windows XP taskbar and select Task Manager from the menu that appears



Task	Status
Jasc Paint Shop Pro	Running
Administrative Tools	Running
Performance	Running

Processes: 18 CPU Usage: 2% Commit Charge: 84664K / 63359

Figure 10-1 Task Manager, Applications tab

The first tab in Task Manager is the Applications tab, which is shown in Figure 10-1. This tab displays all programs currently running on the computer and the status of those programs (usually "Running"). You can use this tab to halt an application by highlighting an entry in the list and clicking the End Task button. To switch to a specific task, highlight an entry and click the Switch To button. To launch a new application, click the New Task button and provide the name of an executable program or command in the Create New Task dialog box that appears.

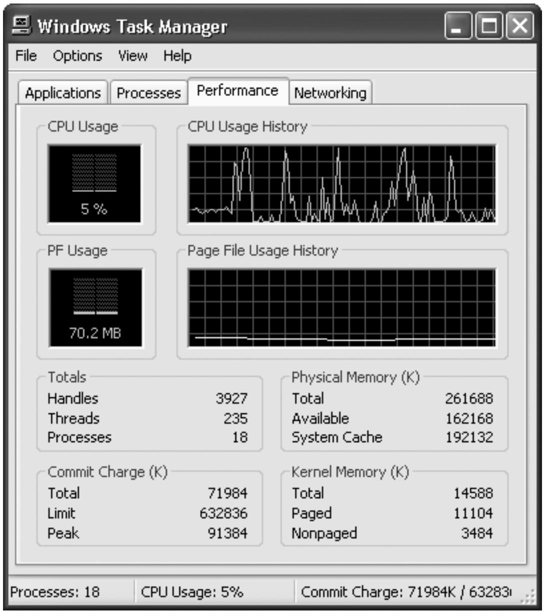
The Processes tab offers information about all currently active processes, including Process ID number (PID), CPU usage (CPU), CPU time, and Memory Usage. A **process** is an environment that defines the resources available to threads, which are the executable parts of an application. This display is an excellent instant diagnostic tool to show when ill-behaved applications take up an inordinate amount of CPU time. If this happens at the moment you use Task Manager, you'll see the process's CPU usage spike above 90%. Even if an application is not currently hogging the CPU, the CPU time entry might be high enough (above 80%) to stick out like a sore thumb.

You can change the columns displayed on the Processes tab by choosing Select Columns from the View menu. The Processes tab lists all processes that contribute to the operation of Windows XP Professional, including Winlogon.exe and Lsass.exe. You can stop any process by selecting it from the list, then clicking the End Process button.

Caution

Be wary of ending Windows XP processes; you can cripple or disable a system by ending processes that are required for proper system operation. That's why Microsoft recommends terminating applications rather than processes. However, sometimes the only way to access a rogue system component is through the Processes tab.

The Performance tab, shown in Figure 10-2, provides a graphical representation of cumulative CPU usage and memory usage. The four text windows at the bottom of the screen provide detailed information on the total number of handles, threads, and processes (Totals) active on the system, the amount of memory allocated to application programs or the system (Commit Charge), the amount of physical memory installed on your computer (Physical Memory), and the memory used by the operating system for internal processes (Kernel Memory). A **thread** is the minimal unit of system execution and corresponds roughly to a task within an application, within the Windows XP Professional kernel, or within some other major system component. A **handle** is an internal identifier for some kind of system resource, object, or other component that must be accessed by name.



CPU Usage: 5 %

PF Usage: 70.2 MB

Totals	
Handles	3927
Threads	235
Processes	18

Physical Memory (K)	
Total	261688
Available	162168
System Cache	192132

Commit Charge (K)	
Total	71984
Limit	632836
Peak	91384

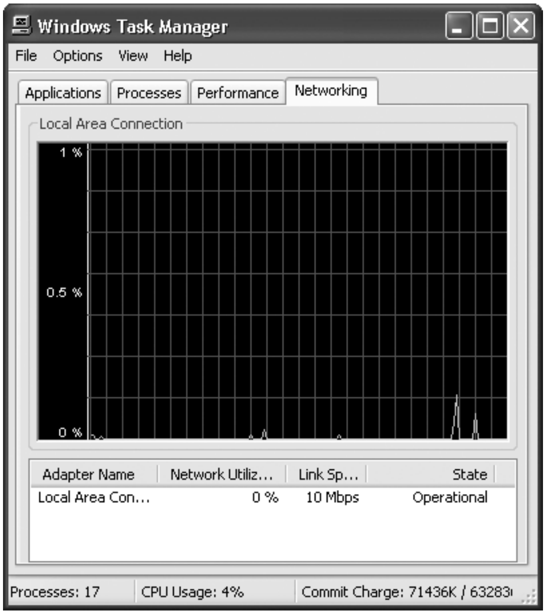
Kernel Memory (K)	
Total	14588
Paged	11104
Nonpaged	3484

Processes: 18 CPU Usage: 5% Commit Charge: 71984K / 63283

Figure 10-2 Task Manager, Performance tab

The Networking tab in Task Manager shows current levels of network utilization, on a per-interface basis, as shown in Figure 10-3. For computers with more than one network interface, you must select a specific Adapter Name in the textbox underneath the utilization graph to view its corresponding chart. Note also that by default the "Auto Scale" option is selected; because the network in view is only lightly utilized, the graph shows only utilizations between 0 and 1 percent.

You can use the Performance tab in Task Manager to ascertain quickly whether a computer is performing optimally. If the total CPU usage shown in the status bar is consistently high—say over 70%—you can use the Processes tab to identify the process that is monopolizing the CPU and take corrective action.

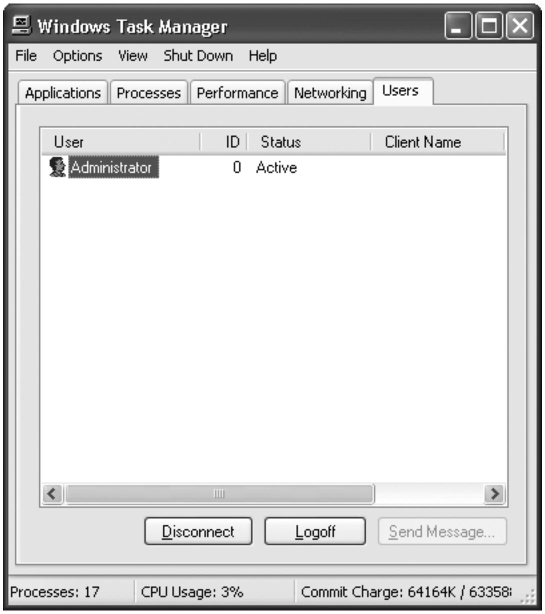


Adapter Name	Network Utiliz...	Link Sp...	State
Local Area Con...	0 %	10 Mbps	Operational

Processes: 17 CPU Usage: 4% Commit Charge: 71436K / 63283

Figure 10-3 Task manager, Networking tab

There is a fifth tab called Users in Task Manager (see Figure 10-4), but it only appears under special circumstances on Windows XP Professional machines. The only machines that have this tab are those that belong to a Windows Workgroup or have been set up to run as standalone machines with no networking capabilities. You must also run the User Accounts utility in Control Panel (Start|Control Panel|User Accounts|Change the way users log on or off) and select the Use the Welcome screen and Use Fast User Switching checkboxes. This facility permits one user to take over a Windows XP machine temporarily (without logging off the other user or changing active applications, settings, and so forth), execute a few commands or a program, and then return control to the original user. This facility is provided as a convenience for home and small office use where multiple users must share a single machine. This facility does not work in a domain environment.


Windows Task Manager
File Options View Shut Down Help
Applications Processes Performance Networking Users
Disconnect Logoff Send Message...

User	ID	Status	Client Name
Administrator	0	Active	

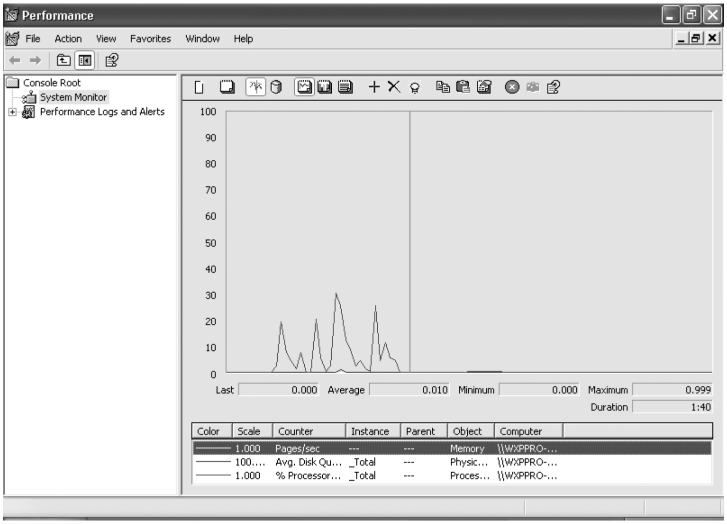
Processes: 17 CPU Usage: 3% Commit Charge: 64164K / 63358

Figure 10-4 Task Manager, Users tab

System Monitor

The performance monitoring tool included with Windows XP Professional can monitor and track many different areas of system performance. Called **System Monitor**, this tool is used to monitor and record the same system measurements as in Windows XP systems (prior to that, the program was called Performance Monitor or Perfmon). As shown in Figure 10-5, System Monitor is a graphical tool that can monitor many different **events** concurrently. By using System Monitor, you can analyze network operations, identify trends and bottlenecks, determine system capacity, notify administrators when thresholds are exceeded, track the performance of individual system devices, and monitor either local or remote computers. To start System Monitor, first open Control Panel through the Start button by selecting Start|Control Panel. Then open Administrative Tools by double-clicking its icon. Finally, double-click Performance to launch the Performance Console, which contains System Monitor. (Hands-on Project 10-1 shows you how to use System Monitor to monitor memory performance.)

The performance tools in Windows XP can perform a wide range of monitoring functions, including real-time monitoring, recording logs for future examination, and generating performance threshold alerts. Through proper use of these functions, system administrators can effectively monitor their systems for bottlenecks, extract historical trends, and receive notification of abnormal activities. All of these uses are discussed in the following sections.



Last 0.000 Average 0.010 Minimum 0.000 Maximum 0.999
Duration 1:40

Color	Scale	Counter	Instance	Parent	Object	Computer
—	1.000	Pages/sec	---	---	Memory	\\WXPPRO-...
—	100....	Avg. Disk Qu...	_Total	---	Physic...	\\WXPPRO-...
—	1.000	% Processor...	_Total	---	Proces...	\\WXPPRO-...

Figure 10-5 System Monitor displays memory pages accessed, disk queue length, and CPU utilization by default

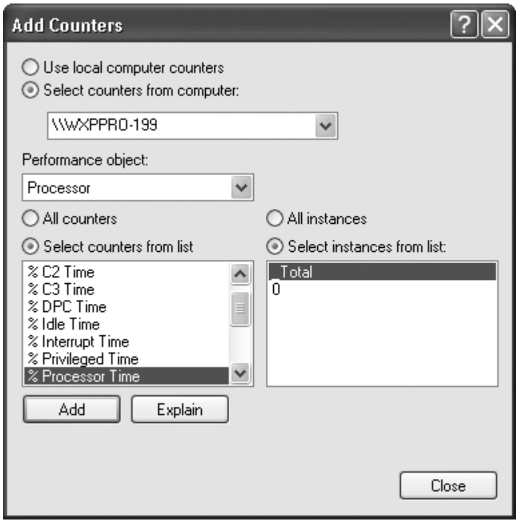
Realtime Monitoring

Realtime monitoring is the process of viewing the measured data from one or more counters in the System Monitor display area. System Monitor can display realtime and logged data in one of three formats: graph (see Figure 10-5), histogram (thermometer bars), or report (text-based instant values). You can select these views or displays by clicking the View Graph (default), View Histogram, or View Report buttons on the toolbar (pop-up windows explain these buttons to you if you leave the cursor over these buttons for more than a second or two).

To begin monitoring a particular counter, click the Add Counters button, which looks like a plus sign on the toolbar. You will see the Add Counters dialog box, shown in Figure 10-6. This dialog box reveals the object-oriented architecture of the Windows XP Professional system as a whole, and of performance monitoring in general. From this dialog box, you select counters based on the following:

- *Local or network-accessible computer*—Counters can be read from the local system or any accessible system over a network.
- *Performance Object*—A **performance object** is a component of the Windows XP Professional system environment that can register with System Monitor for tracking; performance objects range from devices to services to processes.
- *Counter*—Counters are aspects or activities of a performance object that can provide measurable information.

- *Instance*—An **instance** is a selection of a specific performance object when more than one is present on the monitored system; for example, multiple CPUs or hard drives.


Add Counters

○ Use local computer counters
● Select counters from computer:

\\WXPPRO-199

Performance object:

Processor

○ All counters
● Select counters from list

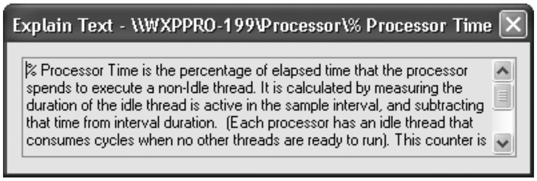
% C2 Time
% C3 Time
% DPC Time
% Idle Time
% Interrupt Time
% Privileged Time
% Processor Time

○ All instances
● Select instances from list:

_Total
0

Figure 10-6 Add Counters dialog box

The Add Counters dialog box also allows you to select all counters for a specific performance object or all instances of a performance object at once. Once you've selected your host computer, object, counter (one or all), and instance (one or all), click the Add button to add the counter(s) and instance(s) to the list. If you need more information on any selected counter, click the Explain button. This reveals a floating window (see Figure 10-7) with additional information about the selected counter. Once you've added all the counters you are interested in monitoring, click Close to return to System Monitor.


Explain Text - \\WXPPRO-199\Processor\% Processor Time

% Processor Time is the percentage of elapsed time that the processor spends to execute a non-Idle thread. It is calculated by measuring the duration of the idle thread is active in the sample interval, and subtracting that time from interval duration. (Each processor has an idle thread that consumes cycles when no other threads are ready to run). This counter is

Figure 10-7 The Explain Text window provides additional information about the counter selected in the Add Counters dialog box

As you'll discover if you spend any time with System Monitor, its counters are numerous. A plain-vanilla Windows XP Professional installation makes it possible to monitor hundreds of such counters. In practice, however, there are only a handful of performance objects and associated counters that you must work with regularly (some more often than others). The following list outlines the performance object and counter pairs that are worth memorizing, as well as several others that you may find useful when evaluating performance on your systems and networks. The list deals with six kinds of objects: LogicalDisk (the divisions of a drive into partitions or dynamic storage units), Memory (RAM), Network, PhysicalDisk (the actual hard disk as a whole), Processor (CPU), and System. For convenience, we present them in alphabetical order, listed in the form *Performance Object: Counter*.

- *LogicalDisk: Current Disk Queue Length*—This counter indicates how many system requests are waiting for disk access. If the queue length is greater than two for any logical drive, that drive is probably suffering from congestion. If you can't redistribute the load across multiple logical disks, consider upgrading your disk subsystem. Always check the corresponding PhysicalDisk counter when examining LogicalDisk counters.
- *LogicalDisk: %Disk Time*—This counter measures the percentage of time that a disk is busy handling read or write requests. It's rare for this percentage to hit 100; it's unusual for this level to be sustained at 80% or higher. If this occurs, redistribute files in an attempt to spread the load across multiple logical drives. Always check the corresponding PhysicalDisk counter.
- *Avg. Disk Bytes/Transfer*—This counter measures the average number of bytes transferred between memory and disk during read and write operations. If the value hovers at or near 4 KB (4086 bytes), this can indicate excessive paging activity on that drive. In general, a larger number indicates more efficient transfers than a smaller one, so look for declines against your baseline.
- *Memory: Available Bytes*—This counter measures the number of bytes of memory available for use on the system at any given moment. Microsoft recommends that this value always be 4096 KB or higher. If values hover at or below this threshold, your system will definitely benefit from additional RAM. You can obtain this number from the Task Manager Performance tab (it's the Available entry in the Physical Memory pane) without having to run System Monitor.
- *Memory: Cache Faults/sec*—This counter measures the number of times that the Windows XP cache manager must ask the system to bring a file's page in from disk or locate it elsewhere in memory. Higher values indicate potential performance problems, because a system's performance is best when cache hit rates are not too high. Establishing a baseline on a lightly loaded system will help you recognize when this counter begins to climb into risky regions (double the values that appear in the baseline or higher). As with monitoring other memory counters, the proper response is to add more memory; in this case, adding more L2 cache is even better than adding main RAM.
- *Memory: Page Faults/sec*—This counter returns the average number of page faults per second for the current processor instance. A page fault occurs whenever a memory page not already loaded in RAM is referenced. When

this happens, the Virtual Memory Manager (VMM) must bring that page in from disk and possibly make room for it by swapping an old page out to disk. Understanding this process helps to explain how memory congestion sometimes manifests itself in excessive disk activity. If this value increases to more than double what you observe in a light-load baseline, it can indicate a need for more RAM.

- *Memory: Pages/sec*—This counter tracks the number of pages written to or read from disk to satisfy requirements of the VMM, and also includes paging traffic for the system cache to access file data for applications. Memory:Pages/sec can indicate that paging levels are slowing the system down. If its number increases to more than double what you observe in a light-load baseline (or, in most instances, goes above 20 for a sustained period of time), there is a strong need for additional RAM.
- *Network Interface: Bytes Total/sec*—This counter presents the total amount of traffic through the computer's network adapter, including all inbound and outbound data (framing characters as well as payload data). When the total amount of traffic begins to approach the practical maximum for the type of media in use—for example, 5.5 Mbps on non-switched 10 Mbps Ethernet—trouble lies ahead, in the form of potential bandwidth saturation. Fixing this problem might require a switch to a faster type of network such as 100 Mbps Ethernet. It may also require the installation of switched Ethernet hubs so that each pair of machines can use the entire 10 Mbps bandwidth that Ethernet can supply when there's no competition for the medium. Another solution is to distribute the machine's load across multiple network segments (and, therefore, multiple adapters) to balance the traffic load.
- *Network Interface: Current Bandwidth*—This measures the current utilization levels of the network medium and provides a background count against which to evaluate the monitored machine's adapter. The same observations about loading and distribution apply to this counter as to Bytes total/sec, except that Current Bandwidth may indicate the need to partition the network to which this machine is attached to lower the total traffic on individual cable segments.
- *Network Interface: Output Queue Length*—This counter keeps track of the number of packets that are queued up for transmission across the network pending access to the medium. As with most other Windows XP queues, if more than two packets are queued, network delays are likely and the bottleneck should be removed, if at all possible.
- *Network Interface: Packets/sec*—This counter monitors the number of packets sent and received across a specific network adapter. Comparison with a baseline indicates when this value is getting out of hand. The observations that apply to the Bytes Total/sec counter also apply to this counter.

- *PhysicalDisk: Current Disk Queue Length*—PhysicalDisk counters track hard disk activity on a per-disk basis and provide much the same kind of information as the LogicalDisk counters. However, calculating acceptable queue lengths for physical disks is different than for logical ones. Here, the threshold for trouble is 2 more than the number of spindles on the hard drive. For ordinary drives this is the same as for logical disks, but for RAID arrays (which Windows 2000 treats as a single drive, but are not supported by Windows XP), the threshold is 2 more than the number of drives in the array.
- *PhysicalDisk: % Disk Time*—This counter records the percentage of time that a hard drive is kept busy handling read or write requests. For Windows XP machines, you may see peaks as high as 100%, but the sustained average should not exceed 80%. High-sustained averages are not worrisome unless the corresponding queue length numbers are in the danger zone as well.
- *PhysicalDisk: Avg. # Disk Bytes/Transfer*—This counter keeps track of the average number of bytes that read or write requests transfer between the drive and memory. Smaller values are more worrisome than larger ones here, because they can indicate inefficient use of drives and drive space. If this behavior is caused by applications, try increasing file sizes. If paging activity is the culprit, an increase in RAM or cache memory is a good idea.
- *Processor: % Processor Time*—This counter tracks the percentage of time that the CPU is busy handling non-idle threads—in other words, doing real work. Sustained values of 85% or higher indicate a heavily loaded machine. Consistent high readings indicate that a machine needs to have its load reduced or its capabilities increased with a new machine, a motherboard upgrade, or a faster CPU. See the "Eight Ways to Boost Windows XP Performance" section later in this chapter for a discussion of these performance improvements.
- *Processor: Interrupts/sec*—This counter calculates the average number of times per second that a device requesting immediate processing interrupts the CPU. Network traffic and system clock activity establish a kind of background count for comparison. Pathological increases occur when a malfunctioning device begins to generate false interrupts or when excessive network traffic overwhelms a network adapter. In both cases, this usually creates a count that's five or more times greater than a lightly loaded baseline.
- *System: Processor Queue Length*—This counter records the number of execution threads that are waiting for access to a CPU. If this value increases to more than double the number of CPUs present on a machine (two for a single-processor system), this machine's load should be distributed across other machines or its capabilities increased, usually by adding an additional CPU or by upgrading the machine or the motherboard. (Increasing CPU speed does not increase performance as much as you might think, because it does nothing for the machine's cache or its memory and bus transfer capabilities.)

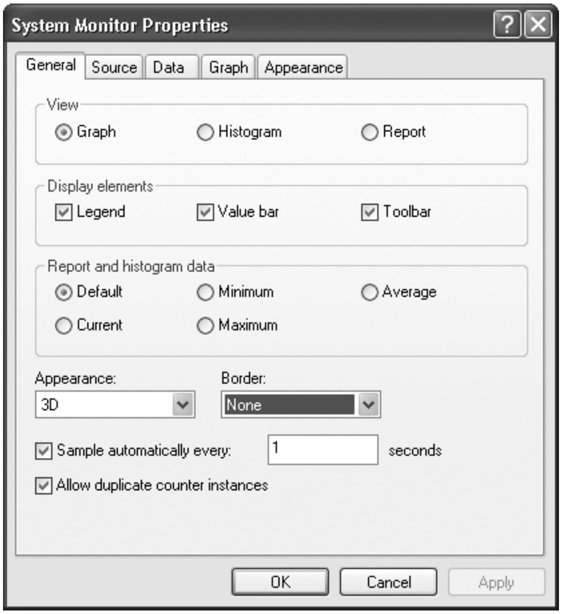
Note

Where we've indicated that more than one counter is worth watching for a particular performance object (for instance, there are four network-related counters), it's more significant when all counters experience a dramatic change in status simultaneously than when only one or two such counters show an increase. Across-the-board changes are more likely to indicate a bottleneck than are more localized changes (because they are more likely to be caused by applications or by shifts in local conditions, traffic levels, and so forth).

You can customize the display of System Monitor through its Properties dialog box. Access the System Monitor Properties dialog box by selecting System Monitor in the left pane, then right-clicking in the right pane and selecting Properties from the resulting menu. Alternately, you can click the Properties button, which looks like a hand holding a piece of paper, in System Monitor's toolbar. The General tab (shown in Figure 10-8) offers the following controls:

- Set the view to Graph, Histogram, or Report (that is, the same function as the toolbar buttons)
- Enable the Legend, Value bar, and Toolbar items
- Set the report and histogram data to Default, Current, Average, Minimum, or Maximum
- Set the appearance to 3D or Flat
- Set the border to None or Fixed Single
- Set the update/measurement interval in seconds; default is one second
- Allow duplicate counter instances

The Source tab (see Figure 10-9) is used to specify whether the displayed information is pulled from real-time measurements, from a Counter log (Counter logs are discussed in the "Logging and Using Logged Activity" section later in this chapter), or from a DSN (data source name) database (if available). If a Counter log is used, you must also define the time range.



System Monitor Properties

General | Source | Data | Graph | Appearance

View
● Graph ○ Histogram ○ Report

Display elements
☑ Legend ☑ Value bar ☑ Toolbar

Report and histogram data
● Default ○ Minimum ○ Average
○ Current ○ Maximum

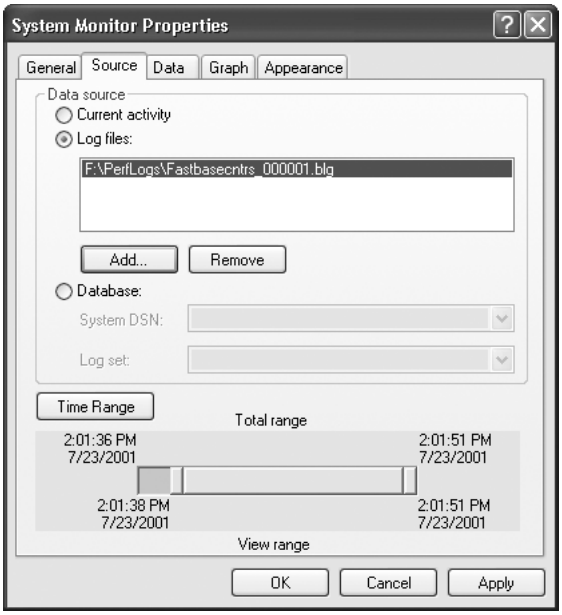
Appearance: 3D
Border: None

☑ Sample automatically every: 1 seconds

☑ Allow duplicate counter instances

OK | Cancel | Apply

Figure 10-8 System Monitor Properties, General tab



System Monitor Properties

General | Source | Data | Graph | Appearance

Data source
○ Current activity
● Log files:
F:\PerfLogs\Fastbasecntrs_000001.blg

Add... | Remove

○ Database:
System DSN:
Log set:

Time Range

Total range
2:01:36 PM 7/23/2001 — 2:01:51 PM 7/23/2001

View range
2:01:38 PM 7/23/2001 — 2:01:51 PM 7/23/2001

OK | Cancel | Apply

Figure 10-9 System Monitor Properties, Source tab

Use the Data tab to add or remove counters and to alter the color, scale, width, and style (all using pull-down lists) for each counter's chart line. The Graph tab defines a title and vertical axis label, enables vertical and horizontal grid lines, indicates whether to display vertical scale numbers, and sets the vertical maximum and minimum scale. The vertical maximum and minimum scales are used to focus or expand the display to make counter measurements more informative. For example, if several counters display measurements within .3 deviations of the 80 mark, setting the maximum to 85 and the minimum to 75 expands the displayed information to grant an order of magnitude of greater detail. The Appearance tab includes a Color pane where you can define the colors for the various components of System Monitor. Likewise, the Font pane on the Appearance tab allows you to choose the font used to display text information. (Try Hands-on Project 10-2 to alter System Monitor display parameters.)

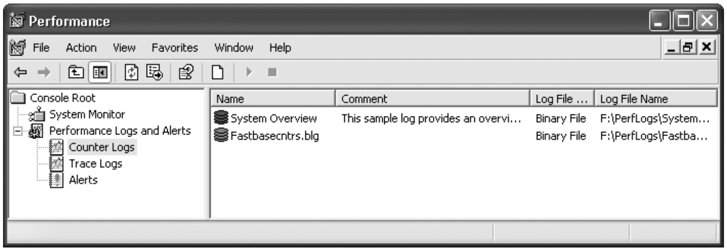
The System Monitor display in Chart (Graph) view (refer to Figure 10-5) can show 100 data points from left to right. As each data point is measured and data is added to the display, the event horizon line moves one point to the right. Below the graph of data in both Chart and Histogram views, five metadata items are listed: the last, average, maximum, and minimum measurements of the selected counter and the total duration of the display field (calculated by multiplying the measurement interval by 100). Below these items is the counter legend, which lists all counters displayed in the graph, along with information about color, scale, counter name, instance, parent, object, and computer source. Selecting a counter in the legend changes the content of the five metadata points.

Report view displays all selected counters grouped by instance, counter, object, and computer in text form. The information displayed in a report is the last measured value when viewing real-time data, or the averaged value over all data points in a time range when viewing logged data.

Logging and Using Logged Activity

The Windows XP Professional Performance tool offers two types of logging capabilities. A **Counter log** records data from selected counters at regular, defined intervals, allowing you to define exactly which counters are recorded (based on computer, performance object, counter, and instance). A **Trace log** records non-configurable data from a designated provider (such as the kernel) only when an event occurs (such as process creation, thread deletion, disk I/O, and page fault). Trace logs are operating system environment status dumps more similar to the memory dump written when a Stop error occurs than a log of performance statistics. You can review Counter log files using System Monitor. Trace logs differ from counter data logs in that they measure data continually rather than taking only periodic samples.

Using Counter logs is fairly simple. First, select the Counter Logs item beneath the Performance Logs and Alerts node of the Performance tool (see Figure 10-10). Notice that a Counter log named System Overview is already defined by default. You can use this predefined Counter log to get a basic look at the performance of the system. It's a basic look because it looks at only three counters—memory, storage, and CPU. Creating your own Counter log requires selecting counters (based on computer, object, counter, and instance), setting the measurement interval, providing file storage information, and setting start and stop times.



Name	Comment	Log File ...	Log File Name
System Overview	This sample log provides an overvi...	Binary File	F:\PerfLogs\System...
Fastbasecntrs.blg		Binary File	F:\PerfLogs\Fastba...

Figure 10-10 The Counter Logs node in the Performance tool is where you configure and access Counter log files

Counter logs record data at regular intervals; all counters in a Counter log use the same interval. The default interval is 15 seconds, but you can define intervals from 1 second to 999,999 days.

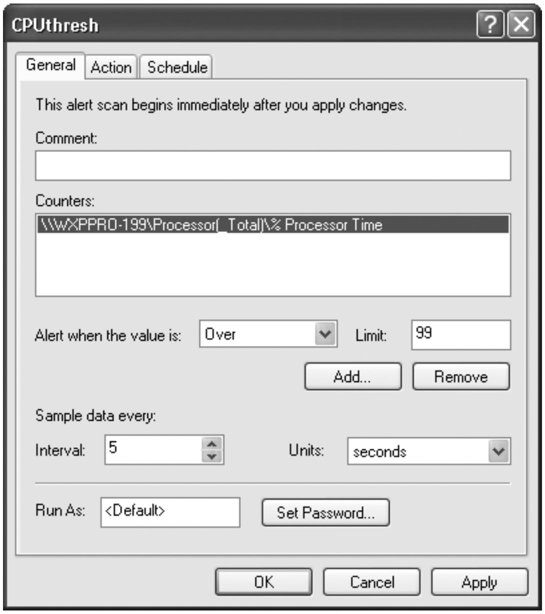
The Properties dialog box for Counter logs has three tabs. The General tab shows the filename of the selected log, lists all counters included in the log, allows adding and removing counters, and sets the measurement interval. The Log Files tab sets the file type (comma-delimited, tab-delimited, binary, or SQL database) and defines the file name extension. By clicking the Configure button, you can change the name and location of the file and set the maximum file size in KB or available drive space. The Schedule tab defines the start and the stop times for the log (either manual or at a specified time). You can terminate a log manually or set termination to occur after a specified length of time, at a specified time, or when the file is full. Once a log file closes, you can run a command (such as a batch file) or start a new log file (if drive space is available).

Once you define a Counter log, you can either wait for the defined start time or issue the Start command from the Action menu to begin recording data. Once you start recording, the Counter log will continue to collect data until you stop the recording manually (by issuing the Stop command from the Action menu) or a defined stop event occurs (such as after a time period, a specific time, or when the log is full). The Counter log records data even when the Performance tool is closed. While a Counter log is recording data, the log icon beside the name will be green. When the recording stops the icon turns red. To learn how to create, start, and stop a Counter log, try Hands-on Project 10-3.

Once you've recorded a log file, it can be used in System Monitor. To do so, open Properties for System Monitor and go to the Source tab (refer to Figure 10-9). Select the Log files radio button, click the Add button, then provide the path to the Counter log file (by default such logs are stored in *%systemroot%*\PerfLogs). Next, click the Time Range button to reveal the start and stop time stamps for the recorded data. Using the sliding endpoints, click and drag the view range. Time Range is used to focus the display around important data. Keep in mind that the display area can reveal only 100 measurement points. If you select more than 100 data points, System Monitor will resample the data down to 100 points. For example, if you have 300 points, every three data items will be averaged to produce a single point. System Monitor retains all 300 data points, but only the average points appear. If fewer than 100 data points are selected in the time range, the data is displayed without any extrapolation. (You can practice viewing data from a Counter log in System Monitor in Hands-on Project 10-4.)

Alerts

An **alert** is an automated watchdog that informs you when a counter crosses a defined threshold, high or low. An Alert object can consist of one or more counter/instance-based alert definitions. For example, you can configure an alert to be sent if the CPU goes above 99% usage, which is a possible indicator of CPU overload (see Figure 10-11). The individual alert definitions within an Alert object share the same sample interval, action triggers, and stop/start settings, but operate as distinct alert events. More than one Alert object can be created to assign different sample rates, action triggers, and stop/start settings.


CPUthresh

This alert scan begins immediately after you apply changes.

Comment:

Counters: \\WXPPRO-199\Processor(_Total)\% Processor Time

Alert when the value is: Over

Limit: 99

Sample data every:

Interval: 5

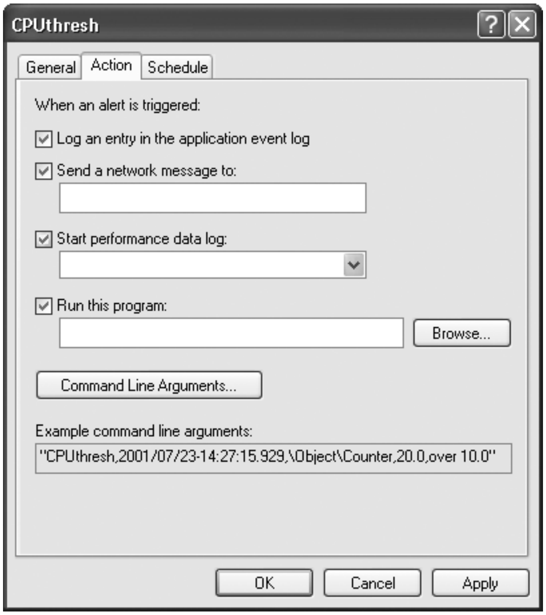
Units: seconds

Run As: <Default>

Figure 10-11 Setting a CPU threshold alert

An alert is defined on a counter/instance basis just like counter selection for the Counter log and System Monitor. An alert definition focuses on one or all counters of one or all objects on the local or networked computer. Each alert definition is assigned a threshold and told whether to issue an alert when the measured value is under or over that threshold. An alert event is triggered only when the measured value of the specific counter at the time of alert sampling has crossed the threshold. Counter levels between samplings have no effect on alerts, because those levels are unknown to the alert monitoring system. The sampling interval of an Alert object is the same as that of Counter Logs—one second to 999,999 days. (Try Hands-on Project 10-5 to create an Alert object.)

When an alert is triggered, any of the following four actions can occur. These are enabled and defined on the Action tab of an Alert object's Properties dialog box, as shown for the "CPUthresh" Alert object in Figure 10-12.



When an alert is triggered:

☑ Log an entry in the application event log

☑ Send a network message to:

☑ Start performance data log:

☑ Run this program:

Example command line arguments:

"CPUthresh,2001/07/23-14:27:15.929,\Object\Counter,20.0,over 10.0"

Figure 10-12 The Action tab controls actions taken for Alert objects when thresholds are passed, or specific events occur

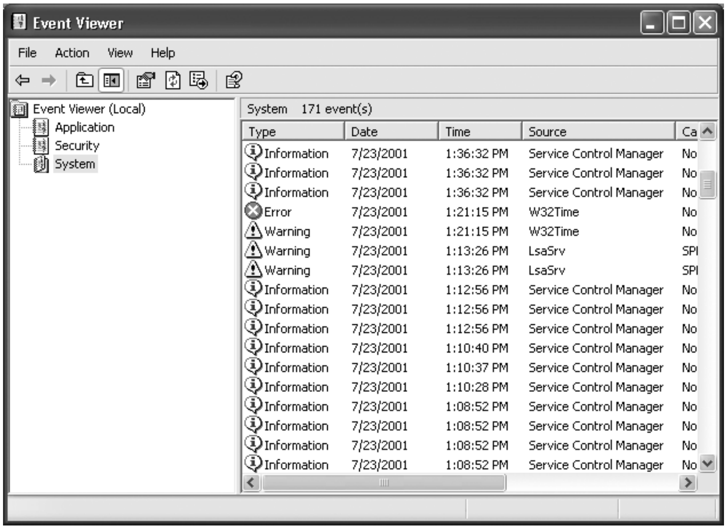
- *Log an entry in the application event log*—You can view the event detail through Event Viewer.
- *Send a network message to*—A single NetBIOS name for a user, group, or computer can be defined. When an alert occurs, a message regarding the alert and the measured counter level is sent to the designated entity.

- *Start performance data log*—Starts the recording of a Counter log.
- *Run this program*—Used to execute a program with command-line options or to launch a batch file. When this action is used, a string of performance-related information can be included at the end of the defined command line in the form. You can choose to have a single argument string with all data points separated with commas, or individual strings with the data elements of date/time, measured value, alert name, counter name, limit value, and a custom text string.

The Schedule tab in an Alert event's Properties dialog box is similar to that for a Counter log. Use this tab to define a start event that is either manual or at a specified time and a stop event that can be manual, after a period of time, or at a specified time. Similar to Counter logs, Alert events function even when the Performance tool is closed.

Event Viewer

The Windows XP Professional **Event Viewer** is another useful tool for examining the performance and activities on a system. The Event Viewer tracks all events generated by the operating system as well as security and application events. An event is anything that causes an event detail to be created in one of the logs that the Event Viewer manages. Failure of a device to load, an unsuccessful logon, or a corrupt database file can all be recorded by Event Viewer and viewed through one of three log files: System, Application, or Security. Access Event Viewer through the Administrative Tools in the Control Panel (try Hands-on Project 10-6). Figure 10-13 shows a typical Event Viewer displaying the System log.



System 171 event(s)

Type	Date	Time	Source	Ca
Information	7/23/2001	1:36:32 PM	Service Control Manager	No
Information	7/23/2001	1:36:32 PM	Service Control Manager	No
Information	7/23/2001	1:36:32 PM	Service Control Manager	No
Error	7/23/2001	1:21:15 PM	W32Time	No
Warning	7/23/2001	1:21:15 PM	W32Time	No
Warning	7/23/2001	1:13:26 PM	LsaSrv	SPI
Warning	7/23/2001	1:13:26 PM	LsaSrv	SPI
Information	7/23/2001	1:12:56 PM	Service Control Manager	No
Information	7/23/2001	1:12:56 PM	Service Control Manager	No
Information	7/23/2001	1:12:56 PM	Service Control Manager	No
Information	7/23/2001	1:10:40 PM	Service Control Manager	No
Information	7/23/2001	1:10:37 PM	Service Control Manager	No
Information	7/23/2001	1:10:28 PM	Service Control Manager	No
Information	7/23/2001	1:08:52 PM	Service Control Manager	No
Information	7/23/2001	1:08:52 PM	Service Control Manager	No
Information	7/23/2001	1:08:52 PM	Service Control Manager	No
Information	7/23/2001	1:08:52 PM	Service Control Manager	No

Figure 10-13 Event Viewer, displaying a typical System log

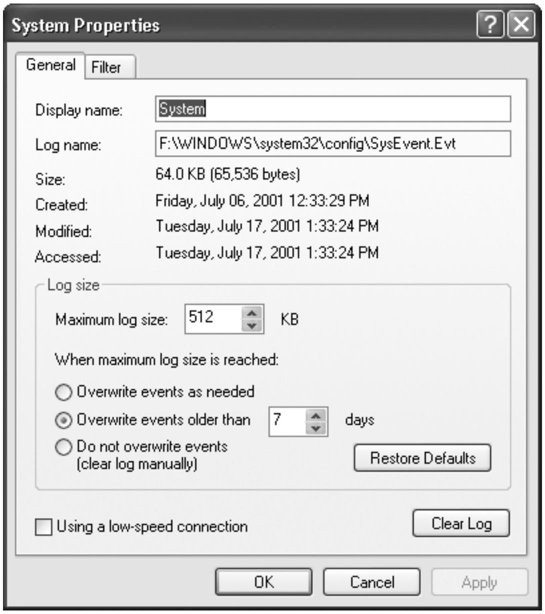
Three types of System and Application log events and two types of Security log events are recorded in Event Viewer, as follows:

- *Information*—Signifies rare but significant events about successful operation of internal services and drivers, indicated by the "i" icon. For example, when a database program loads successfully, it may generate an Information event.
- *Warning*—Signifies potential problems although there is no present danger, indicated by an "!" (exclamation point) icon. For example, if disk space is running low, a Warning event may be logged.
- *Error*—Signifies the presence of significant problems requiring immediate attention, indicated by a white "x" in a red circle. For example, if a driver fails to load correctly, an Error event is issued.
- *Success Audit*—A Security log event that indicates that an event selected for audit has taken place. For example, when a user successfully logs on to a system, a Success Audit event is logged. A gold key icon represents success audits.
- *Failure Audit*—A Security log event that indicates when an audited event has failed. For example, an unsuccessful attempt to access a network drive is logged as a Failure Audit event. A gold lock icon represents failure audits.

The System log is the primary log file for most system services, drivers, and processes. Typical System log events occur when device drivers fail to load or load with errors, when system services fail to start, when system service errors or failures occur, or when auditing is enabled and system-related events flagged for audit occur. The Application log contains event messages that can be generated by Windows XP Professional native applications or services. Unlike the System and Application logs, the Security log does not automatically track events. It records audit events such as logon, resource access, and computer restart and shutdown. Auditing must be enabled and configured (for details see Chapter 6, "Windows XP Security and Access Controls").

All Event log entries include the event's date and time, source, category (such as Logon or Logoff), an event number, the name of the account that generated the event, and the name of the computer on which the event occurred. You can use Event Viewer to view logs on other computers. To access log files on other computers, select the Connect to another computer command in the Action menu while Event Viewer (Local) is highlighted.

Each Event Viewer log has customizable properties. Access a log's Properties dialog box by highlighting that log, then selecting the Properties command from the Action menu. The Properties dialog box (see Figure 10-14) has two tabs. Use the General tab to set properties such as the displayed name, the maximum file size, action to take when log is full (overwrite as needed, overwrite only events older than a specified number of days, or do not overwrite), and whether to manually clean out the log. Use the Filter tab to reduce the number of events displayed. Filter options include sorting by the five event types, source of the event, event category, event ID, user, computer, and date range.



Display name: System

Log name: F:\WINDOWS\system32\config\SysEvent.Evt

Size: 64.0 KB (65,536 bytes)

Created: Friday, July 06, 2001 12:33:29 PM

Modified: Tuesday, July 17, 2001 1:33:24 PM

Accessed: Tuesday, July 17, 2001 1:33:24 PM

Log size

Maximum log size: 512 KB

When maximum log size is reached:

○ Overwrite events as needed

● Overwrite events older than 7 days

○ Do not overwrite events (clear log manually)

□ Using a low-speed connection

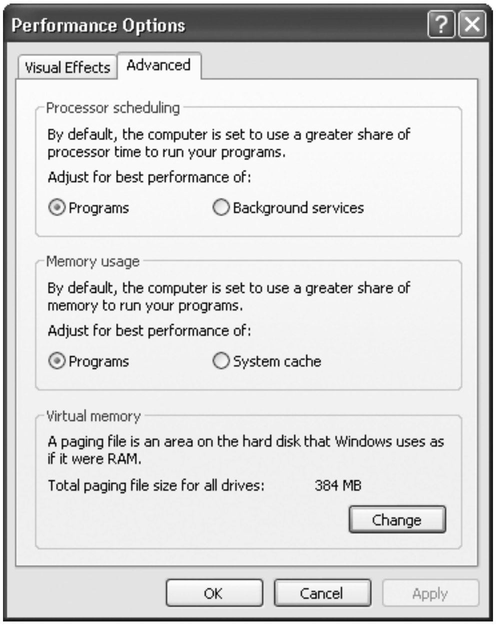
Figure 10-14 System Properties, General tab

Performance Options

You use the Performance Options dialog box (see Figure 10-15) to adjust system performance based on applications and virtual memory. Access this dialog box by clicking the Settings button in the Performance pane on the Advanced tab of the System applet found inside the Control Panel. From there, click the Advanced tab in the Performance Options window. Here you'll find three controls.

First, you can optimize processor scheduling by indicating whether the computer is used primarily for user or interactive programs or background services (the default is programs, as you'd expect for a desktop operating system). The radio button selection of Programs boosts the priority of foreground processes, whereas Background services balances the use of processor resources for foreground and background processes.

Second, you can optimize memory usage in much the same way by indicating whether memory should favor programs or the system cache. The radio button selection of Programs grants more memory to foreground programs; choosing system cache gives the operating system more latitude in managing memory allocations (here again, the default is Programs, as you'd expect for a desktop operating system).



Processor scheduling

By default, the computer is set to use a greater share of processor time to run your programs.

Adjust for best performance of:

● Programs ○ Background services

Memory usage

By default, the computer is set to use a greater share of memory to run your programs.

Adjust for best performance of:

● Programs ○ System cache

Virtual memory

A paging file is an area on the hard disk that Windows uses as if it were RAM.

Total paging file size for all drives: 384 MB

Figure 10-15 The Performance Options dialog box (Advanced tab) offers controls for Processor scheduling, Memory usage, and Virtual memory

Third, you can manage the size of the paging file—that portion of disk space where the operating system stores memory pages not in active use to extend the capacity of memory beyond what physical RAM in the system allows—in the virtual memory pane. In most cases, Windows XP's automatic paging file selection should be adequate, but if System Monitor shows excessive hard page faults, increasing the size of this file (if hard disk space allows) can improve system performance. By default, the paging file size is set between 1.5 and 3.0 times the amount of RAM in the system or 192-384 MB, whichever number is greater.

Use the Change button on the Performance Options dialog box to access the Virtual Memory dialog box, where the size and location(s) of the paging file may be defined. See Chapter 3, "Using the System Utilities" for more details on optimizing paging file sizes.

Setting Application Priority

Windows XP Professional uses 32 levels of application priority, numbered 0 (zero) to 31, to determine which process should gain access to the CPU at any given moment. Users have only minimal control over the initial startup priority level for any launched task. The following list indicates important ranges and specific priority levels:

- 0–15—User-accessible process priorities
- 16–31—System-accessible process priorities

- 0–6—Low user range
- 4—Low value (as set in Task Manager, or with /low parameter to Start command)
- 5—BelowNormal value (as set in Task Manager)
- 7—Normal (default setting for user processes)
- 8–15—High user range
- 10—AboveNormal value (as set in Task Manager)
- 13—High value (as set in Task Manager, or with /high parameter to Start command)
- 16–24—Realtime values accessible to Administrator-level accounts
- 24—Realtime value (as set in Task Manager, or with /realtime parameter to Start command)
- 25–31—Realtime values accessible to operating system only

There are two techniques available to users and administrators to manipulate process priorities: manage already running processes using Task Manager or use the Start command to launch processes with specific priority settings. One reason you may want to manipulate the priority of a process is to give a time-sensitive application priority over another application.

To use Task Manager, right-click any unoccupied region of the taskbar and select Task Manager from the menu. On the Processes tab of Task Manager, select the name of the desired process (usually this is the name of an .exe file that corresponds to the process), then right-click that process to produce another menu. From this menu, select the Set Priority item. This is where you can pick one of the predefined priority settings—Low, BelowNormal, Normal, AboveNormal, High, or Realtime. The current setting is the entry marked with a bullet symbol to the left. You must be logged on with Administrator privileges to use the Realtime setting.

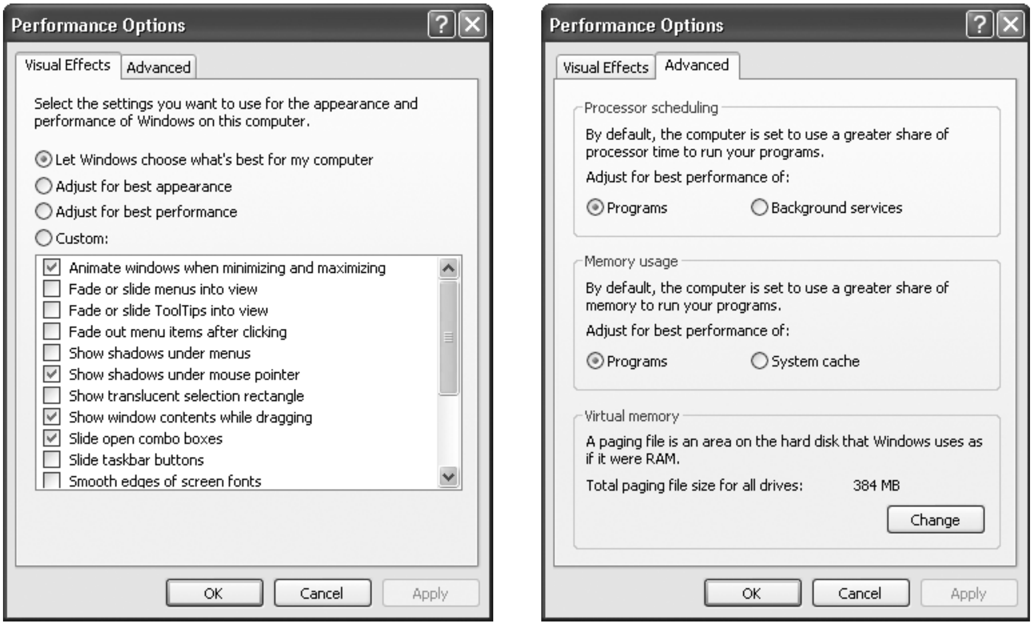
You can use the Start command from a command prompt to launch a new application at some priority level other than the default. You can enter this command from either a command prompt or the Run command. The Start command follows this general syntax:

```
Start /<priority-level> <program>
```

where /<*priority-level*> must be one of /low, /belownormal, /normal, /abovenormal, /high, or /realtime, and <*program*> is a valid path plus filename for the program you want to launch at the specified priority level. For more details on the Start command, enter *start /?* from a command prompt.

Performance Tuning in the System Applet

The System Applet in Control Panel includes an Advanced tab that addresses several Performance entries. To access this utility, follow this menu sequence if you're using the Category View: Start|Control Panel|Performance and Maintenance, then click the System icon in the Control Panel section. The Windows Classic view is simpler: Start|Control Panel|System. Next, select the Advanced tab, then click the Settings button in the Performance pane. You should see a display like the one shown in Figure 10-16, where the Visual Effects tab is selected by default and an Advanced tab is also available, as shown in Figure 10-17.



Performance Options

Visual Effects | Advanced

Select the settings you want to use for the appearance and performance of Windows on this computer.

● Let Windows choose what's best for my computer
○ Adjust for best appearance
○ Adjust for best performance
○ Custom:

☑ Animate windows when minimizing and maximizing
□ Fade or slide menus into view
□ Fade or slide ToolTips into view
□ Fade out menu items after clicking
□ Show shadows under menus
☑ Show shadows under mouse pointer
□ Show translucent selection rectangle
☑ Show window contents while dragging
☑ Slide open combo boxes
□ Slide taskbar buttons
□ Smooth edges of screen fonts

OK | Cancel | Apply

Performance Options

Visual Effects | Advanced

Processor scheduling

By default, the computer is set to use a greater share of processor time to run your programs.

Adjust for best performance of:

● Programs ○ Background services

Memory usage

By default, the computer is set to use a greater share of memory to run your programs.

Adjust for best performance of:

● Programs ○ System cache

Virtual memory

A paging file is an area on the hard disk that Windows uses as if it were RAM.

Total paging file size for all drives: 384 MB

Change

OK | Cancel | Apply

Figures 10-16 and 10-17 The System Applet's performance controls include Visual Effects and Advanced tabs, respectively

The Visual Effects Tab

The Visual Effects tab permits you to control how Windows XP will handle your computer display when managing screen output. By default, the "Let Windows choose what's best for my computer" setting is selected, which permits the computer to trade performance against appearance as the system load increases. You can instruct Windows XP to always "Adjust for best appearance" or to always "Adjust for best performance" if you prefer to lock the system into a completely consistent mode of graphics operation. Finally, for those who love to tweak and tune their systems, the Custom setting permits

16 different visual effects to be manipulated separately. This listing is intended primarily to show the custom settings that Windows enables by default:

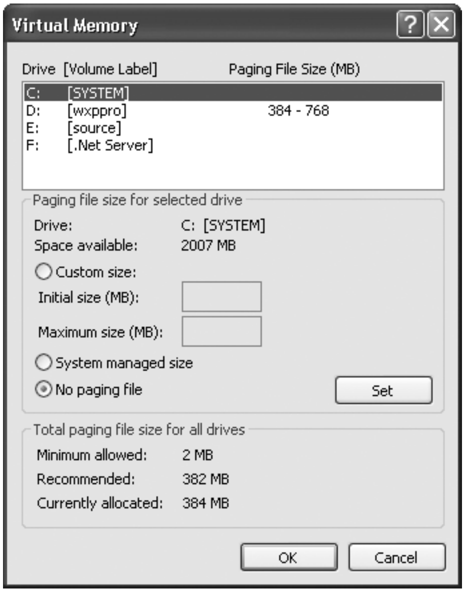
- *Animate windows when minimizing and maximizing*—Shows visual effects when minimization and maximization controls are used.
- *Show shadows under mouse pointer*—Produces a drop shadow beneath the mouse cursor as it moves across the desktop (most noticeable with a dark cursor on a white background).
- *Show window contents while dragging*—As windows are dragged on the desktop, the window outline and some or all of its contents will follow the cursor, where the level of detail displayed depends on the speed of motion and the overall processing load.
- *Slide open combo boxes*—When selecting a menu choice involves picking an item from a list of choices or opening a secondary menu (as is the case with some Start menu elements), the resulting text box is sometimes called a combo box. Enabling this control causes the boxes to slide open from left to right.
- *Smooth-scroll list boxes*—When text boxes contain too many items to fit in the display, you must scroll up or down to view additional elements. Smooth-scrolling means that elements move up or down smoothly, rather than popping one or more list elements up or down at a time. When this control is turned off, lists jump up and down in a more jerky fashion.
- *Use a background image for each folder type*—Associates a more specific image with folders based on their type and contents, rather than using a simpler, more generic icon.
- *Use common tasks in folders*—Drives the task-oriented displays in the left-hand pane of most Windows XP windows and creates the linkage between task data and the window itself to permit that data to be displayed. Disabling this control eliminates display of task information.
- *Use visual styles on windows and buttons*—Instructs Windows XP to use shading, 3-D effects, and edge shading on windows and buttons to give them a more realistic appearance. Disabling this control gives such elements a flat, 2-D appearance.

Although these controls may not seem terribly performance-oriented, keep in mind that drawing the desktop and managing how windows, buttons, and icons appear is a big part of what Windows XP does. By deselecting elements that require more computation or lookup (tasks, visual styles, background images, and so forth) you reduce the burden on the CPU. It won't double the speed of a computer, but it will speed things up somewhat. Notice, for example, that selecting "Adjust for best performance" turns off all settings in the Custom combo box, thereby disabling all visual effects.

The Advanced Tab

The Advanced tab consists of the following three panes:

- *Processor scheduling*—Permits wholesale manipulation of the priority granted to applications versus services. Because Windows XP Professional is a desktop operating system, it should come as no surprise that the default option here is to select "Programs" (applications running on the desktop, presumably at your command) over "Background services" (system and other services usually intended to respond to requests for services from other remote users). This means that the assumption is that most Windows XP machines should prioritize applications over services. Change this setting only on machines where services are not just installed but used regularly by others. This setting routinely boosts the default thread priority for the item chosen by two.
- *Memory usage*—Prioritizes allocating memory to applications rather than to the system cache, again in keeping with Windows XP Professional's primary role as a desktop operating system (where its normal task is to run applications for users). Normally, the System Cache radio button would be selected only on a server or on a desktop machine, where applications themselves require large amounts of system cache (as they would indicate in their documentation or help files).
- *Virtual memory*—By default Windows XP sets its paging file at 1.5 times the amount of RAM installed, with an upper limit of three times that amount. Figure 10-18 shows a default setup on a system with 256 MB of RAM installed (which explains the paging file size of 384-768 MB). The Virtual Memory window can be used to situate and distribute a Windows XP paging file across multiple drives. To achieve maximum performance from a Windows XP paging file, follow as many of these three rules as you can when altering the default setup:
    - Avoid placing the bulk of the paging file on the system and boot partitions whenever possible. If other partitions share a controller with the boot partition, performance benefits will be diminished, because system disk calls and paging calls must use the same disk controller. To enable crash dumps, it remains necessary to create a minimal paging file on the boot partition, the size of which matches the configuration information on the Advanced tab of the System applet (click the Settings button in the Startup and Recovery pane).
    - Spread the paging file across as many drives as possible. If such drives share a controller, performance benefits will be less than if they have separate controllers.
    - There's no performance benefit to spreading paging files across multiple RAID arrays; if you have more than one on your system, you can safely situate the paging file on any single RAID array.


Virtual Memory

Drive [Volume Label] Paging File Size (MB)

Drive	[Volume Label]	Paging File Size (MB)
C:	[SYSTEM]	
D:	[wxppro]	384 - 768
E:	[source]	
F:	[.Net Server]	

Paging file size for selected drive

Drive: C: [SYSTEM]
Space available: 2007 MB

○ Custom size:
Initial size (MB):
Maximum size (MB):
○ System managed size
● No paging file

Total paging file size for all drives

Minimum allowed: 2 MB
Recommended: 382 MB
Currently allocated: 384 MB

Figure 10-18 A Windows XP Professional default setup

Under most circumstances, the defaults for these three settings work nicely on Windows XP machines. Only when the machine acts primarily as a server should the Processor Scheduling and Memory Usage settings be changed. Similarly, only on systems where applications make unusually heavy demands on memory or the operating system should it be necessary to change page file locations and sizes.

Recognizing and Handling Bottlenecks

A **bottleneck** occurs when a limitation in a single component slows down an entire system. The first thing to remember about bottlenecks is that they always exist in any computer. Applications, hard drives, operating systems, and network interfaces might all act as bottlenecks from time to time, but for any given configuration, it is always possible to identify one component that slows the others down the most.

There is no single bottleneck monitor that can easily identify all possible problems. However, by using the monitoring tools included with Windows XP Professional, you can identify possible bottlenecks and make necessary adjustments. The goal when tuning a workstation for performance is to make bottlenecks unnoticeable for everyday functions. A computer used for CAD requires much greater throughput than a computer used primarily for word processing. Ideally, a computer should be waiting for user input rather than making users wait for the computer's response; the user becomes the bottleneck.

Although the details will vary from situation to situation, the process of finding and fixing computer system bottlenecks follows a reasonably consistent course, as shown in the following:

1. Create a baseline for a computer. For Windows XP Professional, this includes observations of memory usage, disk usage, CPU usage, operating system resource usage and activity, and network utilization, at the barest minimum. (See Hands-on Project 10-7 for explicit instructions on creating a sample baseline; you can use the same technique to gather current performance data to compare against an existing baseline.)
2. The first step in identifying potential bottlenecks is to compare baseline observations to current system behavior. In most cases, one or more of the baseline values will have changed for the worse. These changes indicate further areas for investigation.
3. Investigate the more common causes of system problems (some of these for Windows XP Professional are documented later in this chapter) to see if any match the symptoms your computer is exhibiting. If you have a match, the causes of bottlenecks are easy to identify and fixes are easy to apply.
4. If the list of "usual suspects" does not produce an obvious culprit, further analysis is required. You can obtain more details of system behavior from System Monitor and other performance tools, analyze their reports and statistics, and pinpoint potential bottlenecks. Use the general analytical techniques and combinations of objects and counters described in this chapter to help in isolating and identifying bottlenecks.
5. Once a potential bottleneck is identified, you make changes to the system configuration to correct the situation. Sometimes this involves software configuration changes; other times it can involve adding or replacing specific hardware components or subsystems.
6. Always test the impact of any fix you try. Compile a new set of statistics and compare them to the same system measurements before the fix was applied. Sometimes, the fix does the trick and values return to normal, or at least come closer to acceptable levels. If the fix doesn't make a difference, further analysis, other fixes, and more testing are required. It's important to keep at the job until something improves the bottleneck.

It's important to understand that though bottlenecks can always be fixed, some fixes are more expensive than others. Remember, you can always replace an overloaded server or workstation with another bigger, faster system, or you can spread the load from a single overloaded system across multiple systems to reduce the impact on any single machine. These kinds of fixes are a great deal more expensive than tweaking system settings or adding more memory or disk space to a machine. However, in some cases, such drastic solutions are necessary. If you monitor performance correctly, such radical changes needn't take anyone by surprise.

Common Bottlenecks

In this section, we explain how to use the counters you have chosen to watch, either alone or in combination, to determine what kinds of bottlenecks might be present on a system. We also discuss steps you might consider taking to correct such bottlenecks.

Disk Bottlenecks

Disk bottlenecks are the most likely problem when disk-related counters increase more dramatically than other counters (or when compared to your baseline) or when disk queue lengths become unacceptably long. Windows XP Professional collects information about the performance of physical disks (the actual devices) by default.

If Disk Queue Length and % Disk time values remain consistently high (1.5 or higher and more than 80%, respectively), it's probably time to think about adding more disk controllers or drives, or possibly switching existing drives and controllers for newer, faster equivalents (such as UltraWide SCSI or a storage area network, or SAN). This costs money, but can provide dramatic performance improvements on systems with disk bottlenecks. Adding a controller for each drive can substantially improve performance, and switching from individual drives to disk (RAID) arrays can also improve performance on such systems. Because high-end disk controllers often include onboard memory that functions as yet another level of system cache, they can confer measurable performance benefits. But unless users need extremely fast disks for 3D ray tracing, CAD applications, modeling, or other data-intensive applications, this is probably overkill for most conventional desktops.

Software can also contribute to disk bottlenecks through poor design, configuration settings that affect disk performance, or outdated drivers. Because tweaking an application's source code is beyond the reach of most system administrators, inspect the application to see if you can increase the size of the files it manipulates directly or the size of data transfers it requests. Larger and fewer data transfers are faster and more efficient than smaller, more frequent transfers. You should also defragment your hard drives regularly to optimize their performance.

Memory Bottlenecks

Windows XP Professional is subject to various kinds of **memory bottlenecks**. To begin with, it's important to make sure that the paging file is working as efficiently as possible; that is, its size is 1.5 to 3 times the amount of physical RAM on a machine (see Chapter 3). On machines with more than one drive, Microsoft recommends situating the paging file somewhere other than the boot partition (where the Windows system files reside) or the system partition (where the boot loader and other startup files reside). If multiple drives are available, it's a good idea to spread the paging file evenly across all such drives (except a drive with the system or boot partition). Better yet is for each drive to have its own disk controller, which allows Windows XP Professional to access all drives in parallel.

You can detect excessive paging activity by watching the page-related counters mentioned earlier and by observing the lowest number of Available Bytes over time. (Microsoft recommends that this number never dip below 4 MB or 4096 KB.) Excessive disk time and disk queue lengths can often mask paging problems, so be sure to check paging-related statistics when disk utilization zooms. Adding more memory can fix such problems and improve overall system performance.

Processor Bottlenecks

Processor bottlenecks are indicated when the Processor object's % Processor time counter stays consistently above 80% or when the System object's Processor Queue Length counter remains fixed near a value of 2 or more. In both cases, the CPU is being overworked. However, occasional peaks of 100% for processor time are not unusual (especially when processes are being launched or terminated). The combination of consistently high utilization and overlong queues is a more common indication of trouble than an occasional high utilization spike.

Even on machines that support multiple CPUs, it's important to recognize that performance doesn't scale arithmetically as additional CPUs are added. A second CPU gives a more dramatic incremental improvement in performance than a third or fourth; however, two CPUs do not double performance. You're often better off responding to CPU bottlenecks by redistributing a machine's processing load, upgrading its CPU, memory, and motherboard, or replacing the machine altogether. Simply upgrading or adding another CPU neither increases the amount of cache memory on a system nor improves the system's underlying CPU-to-memory data transfer capabilities, both of which often play a crucial role in system performance.

When there is more than one CPU on a system, you can choose to monitor their activity on an individual basis or as a group. To monitor a single CPU, select the individual instance of the CPU. The first CPU is instance 0; the second CPU is instance 1. To monitor the activity of all CPUs as a whole, select the _Total instance.

Network Bottlenecks

Network bottlenecks are not typical on most Windows XP Professional machines, because end users seldom load the network sufficiently to experience performance problems. However, it is worth comparing how much traffic is passing through a workstation's network adapter with the traffic through networking medium to which it is attached. Excessive activity can indicate a failing adapter (sometimes called a "jabbering transceiver") or an ill-behaved application. In both cases, the fix is relatively straightforward—replace the NIC or the application, respectively.

Occasionally, however, the network itself may be overloaded. This situation is indicated by utilization rates that exceed the recommended maximum for the medium in use. (For example, Ethernet should not be loaded more heavily than 56% utilization, but token ring can function adequately at loads as high as 97%.) When this happens, as a network administrator you have two options: divide the network into segments and balance traffic so that no segment is overloaded, or replace the existing network with a faster alternative. Neither of these options is especially fast, cheap, or easy, but the former is cheaper than the latter, and may give your network—and your budget—some breathing room before a wholesale upgrade is warranted.

Eight Ways to Boost Windows XP Professional Performance

Although there are many things you can do to deal with specific system bottlenecks, there are eight particularly useful changes in system components, elements, approaches, or configuration that are likely to result in improved performance by Windows XP Professional. Though these are listed in approximate order of their potential value, all elements on this list are worth considering when performance improvements are needed.

- *Buy a faster machine*—It takes only a year or so for a top-of-the-line, heavily loaded PC to become obsolete these days. When you find yourself considering a hardware upgrade to boost performance, compare the price of your planned upgrade to the cost of a new machine. If you're planning on spending more than half the cost of a newer computer (and can afford to double your expenditure), buy the newer, faster machine. Otherwise, you may be facing the same situation again in a few months. The extra cost buys you at least another year before you must go through this exercise again.

- *Upgrade an existing machine*—You might decide to keep a PC's case, power supply, and some of the adapter cards it contains. As long as the price stays below half the cost of a new machine, replacing a PC's motherboard not only gets you a faster CPU and more memory capacity (both cache and main memory), but it can also get you more and faster bus slots for adapter cards. While you're at it, be sure to evaluate the costs of upgrading the disk controller and hard drives, especially if they're more than twice as slow as prevailing access times. (As we write, garden-variety drives offer average access times of around 8 milliseconds, and fast drives offer average access rates of 2 to 3 milliseconds.)

- *Install a faster CPU*—As long as you can at least double the clock speed of your current CPU with a replacement, such an upgrade can improve performance for only a modest outlay. Be sure to review your memory configuration (cache and main memory) and your disk drives at the same time. A faster CPU on an otherwise unchanged system can't deliver the same performance boost as a faster CPU with more memory and faster drives.

- *Add more L2 cache*—Many experts believe that the single most dramatic improvement for an existing Windows XP PC comes from adding more L2 cache to a machine (or to buy only machines with the maximum amount of L2 cache installed). The CPU can access L2 cache in two CPU cycles, whereas access to main RAM usually takes 8 to 10 CPU cycles. This explains why adding L2 cache to a machine can produce dramatic performance improvements. Although cache chips are quite expensive, they provide the biggest potential boost to a system's performance, short of the more drastic—and expensive—suggestions detailed earlier in this list.

- *Add more RAM*—Windows XP Professional is smart about how it uses main memory on a PC; it can handle large amounts of RAM effectively. It has been widely observed that the more processes that are active on a machine, the more positive the impact of a RAM increase. For moderately loaded workstations (six or fewer applications active at once), 128 MB of RAM is recommended. For heavily loaded workstations, 256 MB or more may improve performance significantly.

Note

When you add RAM to a Windows XP Professional machine, be sure to resize the paging file to accommodate the change properly.

- *Replace the disk subsystem*—Because memory access occurs at nanosecond speeds, and disk access occurs at millisecond speeds, disk subsystem speeds can make a major impact on Windows XP performance. This is particularly true in cases where applications or services frequently access the disk, when manipulating large files, or when large amounts of paging activity occur. Because the controller and the drives both influence disk subsystem speeds, we recommend using only Fast Wide SCSI drives and controllers (or the latest of the EIDE drives and controllers) on Windows XP Professional machines. However, it's important to recognize that a slow disk controller can limit a fast drive and vice versa. That's why upgrading the entire subsystem is often necessary to realize any measurable performance gains.
- *Increase paging file size*—Whenever System Monitor indicates that more than 10% of disk subsystem activity is related to paging, check the relationship between the Limit and Peak values in the Commit Charge pane in Task Manager. (Right-click on any empty portion of the taskbar, select Task Manager, then select the Performance tab and check the lower-left corner of the display.) If the Peak is coming any closer than 4096 KB to the limit, it's time to increase the size of this file. We recommend using a figure somewhere between twice and three times the amount of RAM installed in the machine.
- *Increase application priority*—On machines where a lot of background tasks must be active, you can use the Task Manager's Processes tab to increase the priority of any already running process. Highlight the process entry, then right-click to produce a menu that includes a Set Priority entry. This entry permits you to set the priority to High or Realtime, either of which can improve a foreground application's performance. We recommend that you set only critical applications to Realtime, because they can interfere with the functioning of the operating system. To launch an application with an altered priority level, refer to the section "Setting Application Priority" earlier in this chapter.

Caution

Only users with administrator level access to Windows XP Professional can run processes at a Realtime priority level. Be aware that raising the priority of a single process causes other background processes to run more slowly. The other performance improvements in this list should improve system performance across the board; this improvement affects only those processes whose priorities are increased.

Optimizing Performance for Mobile Windows XP Users

Basically, managing performance for mobile Windows XP machines is substantially the same as managing performance for network-connected Windows XP machines. The same observations about optimizing key system resources—particularly RAM, disk, CPU, and communications—still apply, even though the circumstances will sometimes differ.

Key differences are related to how mobile users access shared resources such as redirected files and IntelliMirror and how they use and synchronize Offline Files. Here, common sense goes a long way. If you follow these simple rules, you'll be able to avoid most potential performance problems that offline or remote use can cause, and you should be able to get the best possible results for your mobile users when they're disconnected from the network:

- Make sure the network interface appears higher in the binding order than a modem or other slower link device. Although users will incur an extra time-out when they fire up a remote link for the first time, once that link is active the delay will disappear. Because network interfaces are much faster than modems, this binding order insures the best overall performance.
- Make sure that file synchronization settings for folder redirection and Offline Files do not require machines to synchronize when running on battery. File synchronization can take a while and can consume significant power. Though some risk may be involved—along with a need for user education about those risks—users working on battery power will generally be happier if shutting down a system or exiting some application does not automatically perform file synchronization.
- Make sure your mobile users understand how to use hibernate and standby modes on their battery-powered machines. It's both faster and significantly less power-consumptive to "wake up" from hibernate or standby mode than it is to reboot from a machine that has been shut down.
- Make sure that all Offline Files a user might need are copied to his or her machine before they leave the network environment. The default is to make local copies only for recently accessed files; under some circumstances, this may not be acceptable—particularly when a slow link is the only way to grab missing items while a mobile users operates off the local network.

- Refresh rates also apply to Group Policy, which defaults to 90 minutes on Windows XP. For machines operating off-network (particularly using modems), refresh rates should be extended to avoid unnecessary network access.
- To prevent file synchronization over slow links, configure group policy's Configure Slow link speed Properties (located in Computer Configuration, Administrative Templates, Network, Offline Files) to define the threshold at which a link is considered slow as opposed to fast. File synchronization will not occur over slow links.

By reviewing how networked machines normally work on a Windows network, and taking the special needs (and slower speeds) associated with remote access or off-network operation into account, you should be able to formulate a series of policies and settings that will help your mobile users obtain the best possible performance when they're not directly attached to their home networks.

Chapter Summary

- Windows XP Professional provides a number of tools to monitor system performance. By using these tools, it is easy to examine the effects of bottlenecks and to improve system response time.
- You can use Task Manager to view applications, processes, and overall system performance, or to stop applications and processes (an efficient way to regain control from an application that is experiencing problems). The default configuration of the Processes tab displays imagename (i.e. processname), user name, CPU, and memory usage. Other columns, such as Virtual Memory Size and Thread count, can be added to the Processes tab.
- The Performance console is an exceptionally useful collection of tools that includes System Monitor, log files, and alerts. System Monitor is used to watch real-time performance or review data collected in log files. Log files record performance data for one or more counters over a specified period of time. Alerts inform administrators when specific counters cross defined threshold levels.
- The Event Viewer is a less dynamic but equally important tool that tracks logs generated by the system. Event Viewer monitors three different logs: System, Application, and Security. The System log records system information and errors, such as the failure of a device driver to load. The Application log maintains similar information for programs, such as database applications. The Security log monitors system security events and audit activities.
- Finally, you should keep an eye on logs and performance counters to isolate any bottlenecks that occur in the system. Once you identify the bottleneck, take the steps necessary to remove it and get the system running more smoothly. In addition, try the recommendations listed in this chapter for improving overall system performance.

KEY TERMS

alert — A watchdog that informs you when a counter crosses a defined threshold. An alert is an automated attendant looking for high or low values, and can consist of one or more counter/instance-based alert definitions.

baseline — A definition of what a normal load looks like on a computer system; it provides a point of comparison against which you can measure future system behavior.

bottleneck — A system resource or device that limits a system's performance. Ideally, the user should be the bottleneck on a system, not any hardware or software component.

counter — A named aspect or activity that the Performance tool uses to measure or monitor some aspect of a registered system or application object.

Counter log — A log that records measurements on selected counters at regular, defined intervals. Counter logs allow you to define exactly which counters are recorded (based on computer, object, counter, and instance).

disk bottleneck — A system bottleneck caused by a limitation in a computer's disk subsystem, such as a slow drive or controller, or a heavier load than the system can handle.

event — A system occurrence that is logged to a file.

Event Viewer — A system utility that displays one of three event logs: System, Security, and Application, wherein logged or audited events appear. The Event Viewer is often the first stop when monitoring a system's performance or seeking evidence of problems, because it is where all unusual or extraordinary system activities and events are recorded.

handle — A programming term that indicates an internal identifier for some kind of system resource, object, or other component that must be accessed by name (or through a pointer). In Task Manager, the number of handles appears on the Performance tab in the Totals pane. A sudden increase in the number of handles, threads, or processes can indicate that an ill-behaved application is running on a system.

instance — A selection of a specific object when more than one is present on the monitored system; for example, multiple CPUs or hard drives.

memory bottleneck — A system bottleneck caused by a lack of available physical or virtual memory that results in system slowdown or (in extreme cases) an outright system crash.

network bottleneck — A system bottleneck caused by excessive traffic on the network medium to which a computer is attached, or when the computer itself generates excessive amounts of such traffic.

performance object — A component of the Windows XP Professional system environment; objects range from devices to services to processes.

object — See performance object.

process — An environment that defines the resources available to threads; the executable parts of an application. Processes define memory available, show where the process page directory is stored in physical memory, and other information that the

CPU needs to work with a thread. Each process includes its own complete, private 2 GB address space and related virtual memory allocations.

processor bottleneck — A system bottleneck that occurs when demands for CPU cycles from currently active processes and the operating system cannot be met, usually indicated by high utilization levels or processor queue lengths greater than or equal to two.

System Monitor — The utility that tracks registered system or application objects, where each such object has one or more counters that can be tracked for information about system behavior.

thread — In the Windows XP Professional runtime environment, a thread is the minimum unit of system execution and corresponds roughly to a task within an application, the Windows XP kernel, or within some other major system component. Any task that can execute in the background can be considered a thread (for example, runtime spell checking or grammar checking in newer versions of MS Word), but it's important to recognize that applications must be written to take advantage of threading (just as the operating system itself is).

Review Questions

1. Monitoring is the act of changing a system's configuration systematically and carefully observing performance before and after such changes. True or False?
2. In a system that is performing optimally, the user should be the bottleneck. True or False?
3. Which of the following can Task Manager monitor?
   a. application CPU percentage
   b. total CPU percentage
   c. process CPU percentage
   d. all of the above
4. The longer a system is in productive use, the more its performance ________________.
5. Which of the following are methods to access Task Manager? (Choose all that apply.)
   a. Ctrl+Alt+Delete
   b. executing "taskman" from the command prompt
   c. Ctrl+Shift+Esc
   d. Control Panel

6. In System Monitor, the counters are the same for all objects. True or False?
7. A(n) ________________ event is issued when a driver fails to load.
8. The ________________ provides a detailed description of a counter.
9. To record log files the Performance tool must be open. True or False?
10. A Counter log can include which of the following?

    a. one or more counters

    b. counters from multiple computers

    c. different intervals for each counter

    d. a stop time defined by a length of time
11. A ________________ occurs when a system resource limits performance.
12. Which of the following objects can be disabled to prevent performance measurements from being taken?

    a. Memory

    b. LogicalDisk

    c. RAS port

    d. System

13. In general, a bottleneck might exist if a queue counter is consistently ________________ than the total number of instances of that object.
14. Which one of the following counters is the most likely indicator of a high level of disk activity caused by too little RAM?

    a. Memory: Pages/sec

    b. Memory: Page Faults/sec

    c. Memory: Cache Faults

    d. Memory: Available bytes
15. Which of the following tools can monitor another computer's information?

    a. System Monitor

    b. Task Manager

    c. Event Viewer
16. The ________________ on the Source tab is used to select a window of data from a Counter log.
17. The ________________ is used to generate system performance reports.

18. What parameter should be used with diskperf to disable only the PhysicalDisk object?
    a. –yd
    b. –yv
    c. –nd
    d. –nv
19. The System Monitor can display only ________________ data points.
20. The ________________ and ________________ event types are available only in the Security log.
21. Of the following commands, which gives the Test.exe application the highest priority level available to ordinary users (not administrators)?
    a. start /abovenormal test.exe
    b. start /normal test.exe
    c. start /high test.exe
    d. start /realtime test.exe
22. Which of the following activities can occur when an alert is triggered?(Choose all that apply.)
    a. an alert to a NetBIOS name
    b. shutdown of the system
    c. start the recording of a Counter log
    d. write an event to the Application log
23. The ________________ feature of Event Viewer can be used to quickly locate all audit details for a specific user.
24. The Start command can be used to alter the priority of active processes. True or False?
25. What change to a system is most effective in producing a performance improvement?
    a. adding RAM
    b. replacing network cables
    c. adding more processors
    d. updating drivers

Hands-on Projects

Project 10-1

To use System Monitor to monitor performance of memory, processor, disks, network, and applications:

1. Open the Control Panel by selecting **Start|Control Panel**.
2. Double-click the **Administrative Tools** icon.
3. Double-click the **Performance** icon.
4. Select the **System Monitor** node in the MMC console.
5. Click **Add** on the toolbar (it's the plus sign).
6. Select the **% Processor Time** counter from the **Processor** object, which is selected by default.
7. Use the Performance object pull-down list to select the **Memory** object.
8. Select the **Pages/sec** counter, if necessary.
9. Click **Add**.
10. Click **Explain**. Read the detail about the selected counter.
11. Repeat steps 7 through 10 to add some or all of the following counters (if multiple instances of these objects are present, select one or more instances and/or the _Total instance):
    - PhysicalDisk: Current Disk Queue Length
    - PhysicalDisk: %Disk Time
    - PhysicalDisk: Avg. Disk Bytes/Transfer
    - Memory: Available Bytes
    - Memory: Cache Faults/sec
    - Memory: Page Faults/sec
    - Memory: Pages/sec
    - Network Interface: Bytes Total/sec
    - Network Interface: Current Bandwidth
    - Network Interface: Output Queue Length
    - Network Interface: Packets/sec
    - Processor: Interrupts/sec
    - System: Processor Queue Length
    - Thread: % Processor Time

- ❐ Thread: Priority Current
- ❐ Process: % Processor Time
- ❐ Process: Elapsed Time
- ❐ Process: Page Faults/sec
- ❐ Process: Thread Count

12. Click **Close**.
13. Launch and close **Windows Explorer** or any other application several times, read files from disk, access network resources, and so on to cause system activity.
14. Notice how the respective lines of the selected counters change according to system activity.

Project 10-2

To use System Monitor to alter the display parameters:

1. Click the **Properties** button on the toolbar (or press Ctrl+Q).
2. Change Sample automatically from every 1 second to **2** seconds.
3. Select the **Data** tab.
4. Select the **\\Memory\Pages/sec** counter.
5. Change the color, width, and style, using the pull-down lists.
6. Select the **Graph** tab.
7. Select the **Vertical grid** and **Horizontal grid** checkboxes.
8. Click **OK** to close the System Monitor Properties dialog box.

Project 10-3

To create, start, and stop a Counter log:

1. Launch the Performance tool if it is not still open from the previous hands-on project.
2. Click the boxed plus sign next to the Performance Logs and Alerts node to expand its contents.
3. Select the **Counter Logs** item.
4. Select **New Log Settings** from the Action menu.
5. Type a name, such as **Set1**. Click **OK**.
6. Click the **Add Objects** button on the General tab, select the **Processor** object in the Performance Objects pane, then click **Add** to add the object, and **Close** to close the window.

Note

You can use this method to select entire objects for monitoring, or you can add counters one at a time. To prevent seeing an error message in step 7, click the Remove button in the Counters list in the Set1 window before proceeding to step 7.

7. Click the **Add Counters** button, select the **% Processor Time** counter in the Select counters from list pane (this is easy; it's selected by default), click the **Add** button to add this counter to the log. Click the **Close** button.
8. Change the Interval from 15 seconds to **2** seconds in the Sample data every textbox.
9. Click **OK** to save your counter log definition. (If you receive an error message, click Yes to create the log now.)
10. Select the **Log Files** tab. Review its controls, but don't make any changes.
11. Select the **Schedule** tab.
12. If you are prompted that the log file path does not exist but can be created, select **Yes** to create the path.
13. In the Start log area, select the **At** option and change the start time to **3** minutes from the present.
14. In the Stop log area, select the **After** option and change the time to **4** minutes.
15. Click **OK**.
16. Notice the new log appears in the list. Within three minutes, its icon will turn green.
17. After the icon turns green, launch and terminate Windows Explorer several times to cause system activity.
18. After four minutes the icon turns back to red. Do not go on with the next hands-on project until the icon is red again.

Hands-on Project

Project 10-4

To view data from a Counter log with System Monitor:

1. Launch the Performance tool if it is not still open from the previous hands-on project.
2. Select the **System Monitor** node.
3. Right-click the right pane and select **Properties** from the resulting menu.
4. Select the **Source** tab.
5. Select the **Log files** option.
6. Use the **Add** button to locate and select the Counter log created in Hands-on Project 10-3. Click **Open**.
7. Click **OK** in the System Monitor Properties dialog box.

8. Click the **New Counter Set** button in the toolbar (the blank page with a sparkle on the top-right corner).
9. Click the **Add** button (the plus sign) on the toolbar.
10. Click **Add** to add the % Processor Counter to the System Monitor display. Note the Counter log recorded in the previous hands-on project has only this one counter so it is selected by default.
11. Click **Close**.
12. Because the Counter log recorded measurements every 2 seconds for 4 minutes, there are 120 data points that are compressed and averaged to create the display you see. To prevent compression of data, you must select a time range of 100 data points or fewer.
13. Click the **Properties** button on the toolbar.
14. Select the **Source** tab.
15. Click the **Time Range** button to refresh the Counter log data.
16. Click and drag the right slider so that only 198 seconds separate the start and stop ends of the view range.
17. Click **OK**.
18. Notice that now 99 data points are displayed.

Project 10-5

To create an Alert object:

1. Launch the Performance tool if it is not still open.
2. Select the **Alerts** node.
3. Select **New Alert Settings** from the Action menu.
4. Type a name such as **Set1**. Click **OK**.
5. Click **Add**.
6. Click **Add** to add the % Processor Time counter to the alert. Note that this counter is selected by default.
7. Click **Close**.
8. Select **Over** in the "Alert when the value is" pull-down box.
9. Type in **50** in the Limit box.
10. Change the sample Interval to **1** second.
11. Select the **Action** tab.
12. Select the **Send a network message to** checkbox.
13. Type in the username of the account with which you are currently logged on.
14. Select the **Schedule** tab.

15. Select the **Manually (using the shortcut menu)** option in the Start scan area.
16. Click **OK**.
17. Select the new **Alert object** that appears in the list of alerts.
18. Select the **Start** command from the Action menu. Its icon will be green when active.
19. Launch and terminate Windows Explorer several times to force system activity. When the % Processor Usage crosses the 50 percent threshold, a network message will appear on your screen. Click **OK** to close it.
20. Select the **Delete** command from the Action menu. Click **OK** to confirm the deletion. This deletes the Action object.

Project 10-6

To use Event Viewer to view an event detail:

1. Open the Control Panel by selecting **Start|Control Panel**.
2. Open the **Administrative Tools** by double-clicking its icon in the Control Panel.
3. Open **Event Viewer** by double-clicking its icon in the Administrative Tools window.
4. Select the **Application log**.
5. Locate and select an Information detail with a SysmonLog source.
6. Double-click the item to open the event detail.
7. Notice that the Description includes information about the counter and the measured level that caused the alert.
8. Click **OK**.
9. Close Event Viewer.

Project 10-7

To create and view a baseline:

1. Open the Control Panel by selecting **Start|Control Panel**.
2. Double-click the **Administrative Tools** icon.
3. Double-click the **Performance** icon.
4. Click the boxed plus sign next to the Performance Logs and Alerts node to expand its contents.
5. Select the **Counter Logs** item.
6. Select **New Log Settings** from the Action menu.
7. Type a name, such as **Baseline1**. Click **OK**.
8. Click the **Add Counters** button on the General tab.
9. Click **Explain** to open the Explain Text window.

10. Use the **Performance object** pull-down list to select the **Memory** object.
11. Select the **Pages/sec** counter in the list under the **Select counters from list** radio button.
12. Read the details in the Explain Text window about the selected counter.
13. Click **Add**.
14. Repeat steps 10 through 13 to add some or all of the following counters (if multiple instances of these objects are present, select one or more instances and/or the _Total instance):
    - PhysicalDisk: %Disk Time
    - Memory: Available Bytes
    - Network Interface: Bytes Total/sec
    - Processor: % Processor Time
    - System: Processor Queue Length
15. Click **Close**.
16. Change the Interval from 15 seconds to **30** seconds.
17. Select the **Log Files** tab. Review its controls, but don't make any changes.
18. Select the **Schedule** tab.
19. If you are prompted that the log file path does not exist but can be created, select **Yes** to create the path.
20. In the Start log area, select the **At** option and change the start time to 3 minutes from the present.
21. In the Stop log area, select the **After** option and change the time to **2** days.
22. Click **OK**.
23. Notice the new log appears in the list. Within three minutes, its icon will turn green.
24. After the icon turns green, continue performing normal or typical work on this system until two days has passed.
25. After one day the icon turns back to red. Do not go on with the remaining part of this hands-on project until the icon is red again.
26. Select the **System Monitor** node in the Performance tool.
27. Right-click the **right pane** and select **Properties** from the resulting menu.
28. Select the **Source** tab.
29. Select the **Log files** option.
30. Use the **Add** button to locate and select the Counter log created in step 7. Click **Open**.
31. Click **OK** in the System Monitor Properties dialog box.

32. Click the **New Counter Set** button in the toolbar (the blank page with a sparkle on the top-right corner).
33. Click the **Add Counters** button (the plus sign) on the toolbar.
34. Use the Performance object pull-down list to select the **Memory** object.
35. Select the **Pages/sec** counter in the list under the Select counters from list radio button.
36. Read the details in the Explain Text window about the selected counter.
37. Click **Add**.
38. Repeat steps 34 through 38 to add some or all of the following counters (if multiple instances of these objects are present, select one or more instances and/or the _Total instance):
    - PhysicalDisk: %Disk Time
    - Memory: Available Bytes
    - Network Interface: Bytes Total/sec
    - Processor: % Processor Time
    - System: Processor Queue Length
39. Click **Close**.
40. Click the **View Report** button from the toolbar. The values listed are an average of all measurements over the entire time period recorded in the log file.
41. Click the **Properties** button on the toolbar.
42. Select the **Source** tab.
43. Click the **Time Range** button to refresh the Counter log data.
44. Click and drag the right and left sliders so that they encompass a time period of 8 hours, such as 9 AM to 5 PM.
45. Click **OK**.
46. Notice that new averaged data points are displayed.
47. Take note of the values seen here, be sure to indicate the time range used for each measurement.
48. Repeat steps 41-47 for the time ranges of 5 PM to 10 PM, 10 PM to 6 AM, 6 AM to 9 AM, and then hourly for each hour of the typical work day (i.e., 9 AM to 10 AM, then 10 AM to 11 AM, etc.)
49. Click the **File** menu, then select **Save As**.
50. Using the Save As dialog box, select a folder and provide a filename to save the console configuration, such as **baseline view1.msc**. Click **Save**.
51. Close the Performance tool by clicking the **File** menu, then clicking **Exit**.
52. At a later date, re-open the Performance tool (see steps 1 through 3).

53. Click the **File** menu, then select **Open**.
54. Using the Open dialog box, locate and select the file saved in step 50. Click **Open**.
55. The view should return to that seen in your final action of step 48.
56. The saved data in the first counter log is your baseline. To use the baseline, you must record a new log file over a similar time period, and compare the new data points with the old data points.
57. Click the boxed plus sign next to the Performance Logs and Alerts node to expand its contents.
58. Select the **Counter Logs** item.
59. Click to select the counter log created in step 7.
60. Right-click over this counter log and select **Properties** from the pop-up menu.
61. Select the **Log Files** tab. Notice the Start numbering at field has been incremented.
62. Repeat steps 18 through 48.
63. Compare the measurements you wrote down from the first baseline Counter log with the most resent Counter log. Any discrepancies may Indicate a change In system activity or may point toward a developing bottleneck.

Case Projects

1. Performance on a Windows XP Professional system used by the accounting department has been slowly degrading. You recently added a 100-Mbps network card, thinking that would correct the problem. To your knowledge, no other hardware has been added to the server, but you suspect someone has been adding software.

   Describe the steps you will use to determine what is causing the system to slow down, including which monitoring applications you will use and on which computer they will be run.

2. You are considering upgrading your Windows XP Professional hardware, including memory, hard drive controller, and video card. The only things you are planning to keep are your hard drive, motherboard, and CPU.

   Outline the tools and utilities you will use to measure the performance increase or decrease, as each new component is added. Include information on expected performance changes and actual changes.